

IN THE CLAIMS:

Please substitute the following claims for the pending claims with the same number:

1 12 (currently amended) A method for limiting the operational life of software in
2 a network environment, the method comprising:
3 providing a program applet [[embedded]] with [[an associated]] a
4 password embedded therewithin to a client computer via a network;
5 receiving from said program applet via said network a request for
6 information stored in a restricted access storage area of a server computer;
7 [[further]] automatically receiving from said program applet said
8 [[associated]] embedded password without manual entry of the password by a user,
9 for authentication;
10 authenticating said [[associated]] embedded password by the
11 server computer and not by the program applet;
12 thereafter providing said information to said program applet via
13 said network while said [[associated]] embedded password is valid; and
14 invalidating said embedded password coincident with an
15 invalidation event.

1 13. (currently amended) A method according to claim 12 wherein said
2 invalidating comprises invalidating said [[associated]] embedded password at a
3 predetermined time.

1 14. (currently amended) A method according to claim 12 wherein said
2 invalidating comprises invalidating said [[associated]] embedded password after
3 lapse of a predetermined [[elapsed]] time from when said request was received.

1 15. (currently amended) A method according to claim 12 wherein said
2 invalidating comprises invalidating said [[associated]] embedded password upon
3 the detection of a loss of communication with said client.

1 16. (canceled)

1 17. (canceled)

1 18. (currently amended) A method according to claim 12 wherein said providing
2 comprises generating said [[associated]] embedded password [[at a server upon
3 receiving said request at said server]].

1 27 (currently amended) A network-based software authentication system
2 comprising a server computer, the server computer comprising:

3 a password generator;
4 password validation apparatus;
5 a restricted-access storage area;
6 a program applet; and
7 invalidation apparatus;

8 wherein said server is operative to:

- 9 a) cause said password generator to generate a password;
10 b) embed said password within said program applet, and provide
11 said program applet [[embedded]] with said password embedded therewithin to a
12 client via a network;
13 c) receive a request for information and automatically receive
14 said embedded password, from said program applet via said network, for
15 authentication, without manual entry of the password by a user[[, from said
16 program applet via said network]];
17 d) authenticate said embedded password using said password
18 validation apparatus and not by said program applet;
19 e) provide said information to said program applet via said
20 network while said [[associated]] embedded password is valid; and
21 f) invalidate said embedded password using said invalidation
22 apparatus coincident with an invalidation event.

1 23. (original) A system according to claim 27 wherein said invalidation event
2 comprises the arrival of a predetermined time.

1 29. (currently amended) A system according to claim 27 wherein said
2 invalidation event comprises the [[elapsing]] lapsing of a predetermined
3 [[elapsed]] time from when said request was received.

1 30. (original) A system according to claim 27 wherein said invalidation event
2 comprises the detection of a loss of communication with said client.

1 31. (canceled)

1 32. (canceled)

1 33 (original) A system according to claim 27 wherein said password is generated
2 at said server computer [upon receiving said request at said server]].